COMMONWEALTH OF VIRGINIA

Information Technology Resource Management Standard

Removal of Commonwealth Data from Electronic Media Standard

Virginia Information Technologies Agency

ITRM Publication Version Control

ITRM Publication Version Control: It is the User's responsibility to ensure they have the latest version of this ITRM publication. Questions should be directed to VITA's Director for Policy Practice and Architecture (PPA) within the Information Technology Investment and Enterprise Solutions (ITIES) Directorate. PPA will update the revision table and issue an email announcement to the Agency Information Technology Resources (AITRs) and Information Security Officers (ISOs) at all state agencies and institutions as well as other parties PPA considers interested in the change.

This chart contains a history of this ITRM publication's revisions.

Version	Date	Purpose of Revision
Original	N/A	Base Document
Revision 2.1.0	10/28/2003	SEC2003-02-1 Rev 0 (10/28/2003)
Revision 2.1.1	03/08/2004	Supersedes SEC2003-02-1 Rev 0
Revision 3	3/15/2008	Supersedes SEC2003-02-1 Rev 1. This revision reflects legislative changes that expanded the CIO's information security responsibilities to include Judicial, Legislative and Independent Agencies branches of government, and Institutions of Higher Education. In addition, appendix B (Non-Disclosure Agreement) and appendix C (Data Removal Quality Assurance Form) along with several minor changes were made to reflect current industry practices and to amplify requirement statements. Also this change reflects the new numbering structure for all PSGs. Changes to this standard are in "BLUE" text with a "legal blackline" in the left margin next to the text location.

Review Process

Technology Strategy and Solutions Directorate Review

N. Jerry Simonoff, VITA Director of Information Technology Investment and Enterprise Solutions (ITIES), and Chuck Tyger, Director, Policy, Practices, and Architecture Division (PPA) provided the initial review of the standard.

Agency Online Review

The standard was posted on VITA's Online Review and Comment Application (ORCA) for 30 days. All agencies, stakeholders, and the public were encouraged to provide their comments through ORCA. All comments were carefully evaluated and the individual commenters were notified of the action taken.

Preface

Publication Designation

COV ITRM Standard SEC514-03 Rev 3

Subject

Removal of Commonwealth Data from Electronic media

Effective Date

March 15, 2008

Supersedes

COV ITRM Standard SEC2003-02.1 March 8, 2004, Revision 1

Scheduled Review

One (1) year from effective date

Authority

Code of Virginia, §§ 2.2-2005 – 2.2-2032.
(Creation of the Virginia Information Technologies Agency; "VITA"; Appointment of Chief Information Officer [CIO])

Code of Virginia, §2.2-2457
(Information Technology Investment Board)

Code of Virginia, §2.2-3800
(Government Data Collection and Dissemination Practices Act)

Scope

This standard is applicable to the Commonwealth's executive, legislative, and judicial branches, and independent agencies and institutions of higher education (collectively referred to as "Agency" that surplus, transfer, trade-in, otherwise dispose of, or replace electronic media resources in the Commonwealth. This standard also applies to equipment owned or leased by the agency. The heads of State agencies, the heads of their field offices, and the heads of institutions of higher education are responsible for compliance with this standard. However, academic "instruction or research" systems are exempt from this standard provided they are not subject to a State or Federal Law/Act mandating security due diligence. This standard is offered only as guidance to local government entities.

Purpose

1) To define the minimum requirements for the removal of Commonwealth data from electronic media resources prior to its being surplused, transferred, traded-in, disposed of, or replaced.
2) To prevent unauthorized use or misuse of state information, and promote the privacy and security of sensitive and/or confidential information resources within the Commonwealth.
3) To comply with federal regulations dealing with the confidentiality of personally identifiable information. Included are regulations such as the Health Insurance Portability and Accountability Act, the Gramm-Leach-Bliley Act (aka, Financial Services Modernization Act), IRS 1075 and the Family Educational Rights and Privacy Act.

Objectives

- Promulgate the minimum requirements for the removal of Commonwealth data from electronic media resources prior to its being surplused, transferred, traded-in, disposed of, or replaced.
- Define a process to certify the removal of Commonwealth data from its electronic media.
- Define a quality assurance process to periodically assess the effectiveness of the removal of Commonwealth data from electronic media.

General Responsibilities

Italics indicate quote from the Code of Virginia requirements)

Information Technology Investment Board (ITIB)

In accordance with *Code of Virginia,* §2.2-2457, the Information Technology Investment Board (the Board) *"is established as a supervisory board, within the meaning of § 2.2-2100, in the executive branch of state government. The Board shall be responsible for the planning, budgeting, acquiring, using, disposing, managing, and administering of information technology in the Commonwealth".*

Virginia Information Technologies Agency (VITA)

In accordance with the *Code of Virginia* §§ 2.2-2005 – 2.2-2032, the Virginia Information Technologies agency (VITA) is assigned the following duties: "*Develop adopt policies, standards, and guidelines for managing information technology by state agencies and institutions.*"

Chief Information Officer of the Commonwealth

In accordance with *Code of Virginia,* § 2.2-2009, the Chief Information Officer (CIO) is assigned the following duties: "*the CIO shall direct the development of policies, procedures and standards for assessing security risks, determining the appropriate security measures and performing security audits of government*

electronic information. Such policies, procedures, and standards will apply to the Commonwealth's executive, legislative, and judicial branches, and independent agencies and institutions of higher education. The CIO shall work with representatives of the Chief Justice of the Supreme Court and Joint Rules Committee of the General Assembly to identify their needs."

Chief Information Security Officer

The Chief Information Officer (CIO) has designated the Chief Information Security Officer (CISO) to develop Information Security policies, procedures and standards to protect the confidentiality, integrity, and availability of the Commonwealth's information assets.

All State Agencies

Agencies are responsible for complying with COV ITRM policies and standards and consider COV ITRM guidelines.

Definitions

Removal of Commonwealth data: Removal of Commonwealth data from electronic media is the process of removing programs or data files on electronic media in a manner that gives assurance that the information cannot be recovered.

Related COV ITRM Policies, Standards, and Guidelines

ITRM Policy SEC500-02: Information Security Management Policy (Revised 07/01/2007)

ITRM Standard SEC501-01: Information Technology Security Standard (Revised July 1, 2007)

ITRM Standard SEC511-00: Information Technology Standard Using Non-Commonwealth Owned Computing Devices to Telework (effective July 1, 2007)

Table of Contents

Background

The surplusing, transfer (including reassignment within the agency), trade-in, disposal, or replacement of electronic media can create information security risks for the agency. This standard applies to all electronic media that has memory such as the hard drives of personal computers, servers, mainframes, Personal Digital Assistants (PDAs), routers, firewalls, switches, tapes, diskettes, CDs, DVDs, cell phones, printers, and Universal Serial Bus (USB) data storage devices.

The risks are related to potential violation of software license agreements, unauthorized disclosure of information such as personally identifiable information, trade secrets, copyrights, and other intellectual property that might be stored on the electronic media. All electronic media containing Commonwealth data, whether stored on Commonwealth assets or that of a service provider, shall have all of that Commonwealth data securely removed from the electronic media as specified by this standard before the electronic media is surplused, transferred, traded-in, otherwise disposed of, or replaced.

Removal of data in the past might have been accomplished by using the FORMAT command or the DOS FDISK command. Ordinarily, using these procedures gave users a sense of confidence that their data had been completely removed. When using the FORMAT command, Windows displays a message such as:

> *Important: Formatting a disk removes all information from the disk.*

The FORMAT utility creates a new FAT or root tables, leaving all previous data on the disk untouched. Moreover, an image of the replaced FAT and ROOT tables are stored, so that the UNFORMAT command can be used to restore them. FDISK merely cleans the PARTITION TABLE (located in the drive's first sector) and does not remove anything else.

In recent years advances in data recovery have been made such that data can be reclaimed in many cases from hard drives that have been wiped or cleared. Free and commercial software exists that use techniques such as Partial Response Maximum Likelihood (PRML), Magnetic Force Microscopy (MFM) and other recovery methods based on patterns in erased bands to recover cleared data.

Approach

Failure to effectively remove the Commonwealth data could result in a violation of laws and regulations including but not limited to the Gramm-Leach-Bliley Act (GLBA), the Health Insurance Portability and Accountability Act of 1996 (HIPAA), The Family Educational Rights and Privacy Act (FERPA), IRS 1075.

This standard also applies to all electronic media owned or leased by the agency or utilized by a service provider. All electronic storage media shall have all Commonwealth data properly removed prior to surplusing, transfer, trade-in, disposal, or replacement. Data removal procedures shall be properly documented in accordance with the processes outlined below in sections B, C and D, and in accordance with the software manufacturers' guidelines to prevent unauthorized release of information that may be stored on electronic media.

Statement of ITRM Requirements for the Removal of Commonwealth Data from Electronic Media

A. General Data Removal Steps

The following steps shall be followed by all agencies and their service providers as well as their remote offices when electronic media is surplused, transferred, traded-in, disposed of, or replaced. The following standards also apply to contractor-supplied electronic media.

A.1 General Steps

a) Before electronic media is surplused, transferred (include reassignment within the agency), traded-in, disposed of, or replaced, all data must be completely erased or otherwise made unreadable in accordance with this standard; however, only after the data has been reviewed and processed for retention in accordance with the agency's records retention policy,

b) All program and data files on any electronic media must be completely erased or otherwise made unreadable in accordance with this standard unless there is specific intent to transfer the particular software or data to the purchaser/recipient.

c) Electronic media shall be securely erased at the earliest time after being taken out of use but not later than 60 days.

d) Whenever licensed software is resident on any electronic media being surplused, transferred, traded-in, disposed of, or replaced, the terms of the license agreement shall be followed.

e) The effectiveness of the data removal process shall be tested by a quality assurance function independent of the organizational unit performing the data removal.

f) After the removal of Commonwealth data from the electronic media is complete, the process shall be certified, as specified below, and a record maintained as specified by the agency's records retention schedule.

B. Hard Drive Data Removal Methods

The following section outlines the acceptable methods to remove data from hard drives. Removal of Commonwealth data shall be performed on hard drives to ensure that information is removed from the hard drive in a manner that the data cannot be recovered. Before the removal process begins, the computer shall be disconnected from any production network to prevent accidental damage to the network operating system or other files on the network. For media going to surplus all identifying tags such as asset inventory tags or licensing information must be completed as outlined in Section F.

B.1 Acceptable Methods

There are three acceptable methods to be used for the hard drives:

- Overwriting – Overwriting is an approved method for removal. Overwriting of data means replacing previously stored data on a drive or disk with a predetermined pattern of meaningless information. This effectively renders the data unrecoverable, but the process shall be correctly understood and carefully implemented.

- Degaussing – Degaussing is a process whereby the magnetic media are erased, (i.e., returned to a zero state). Degaussing (demagnetizing) reduces the magnetic flux to virtual zero by applying a reverse magnetizing field. Properly applied, degaussing renders any previously stored data on magnetic media unreadable.

- Physical Destruction – Hard drives should be physically destroyed when they are defective or cannot be economically repaired or when Commonwealth data cannot be removed. Physical destruction shall be accomplished to an extent that precludes any possible restoration of the data.

The method used for removal of Commonwealth data, depends upon the operability of the hard drive:

- Operable hard drives that will be reused shall be overwritten prior to disposition. If the operable hard drive is to be removed from service completely and has no value for surplus, it shall be physically destroyed or degaussed.

- If the hard drive is inoperable or has reached the end of its useful life, it shall be physically destroyed or degaussed.

Clearing data (deleting files) removes information from electronic media in a manner that renders it unreadable unless special utility software or techniques are used to recover the cleared data. However, because the clearing process does not prevent data from being recovered by technical means, it is **not** an acceptable method of removing Commonwealth data from agency or service provider hard disk storage media.

B. 2 Overwriting

Overwriting is an approved method for the removal of Commonwealth data from hard disk drives. Overwriting of data means replacing previously stored data on a drive or disk with a predetermined pattern of meaningless information. This effectively renders the data unrecoverable. The overwriting process including the software products and applications used for the overwriting process shall include the following steps:

a) The data shall be properly overwritten with pseudo random data by means of, at a minimum, one pass of the entire device for a 15 gigabyte or greater

drive. A minimum of three passes of pseudo random data must be applied to drives smaller than 15 gigabytes in size.

b) The software shall have the capability to overwrite the entire hard disk drive, independent of any BIOS or firmware capacity limitation that the system may have, making it impossible to recover any intelligible data.

c) The software shall have the capability to overwrite using a minimum of one pass or three passes of pseudo random data on all sectors, blocks, tracks, and any unused disk space on the entire disk medium.

d) The software or supporting software shall have a method to verify that all data has been removed. Verification must be performed to verify that each drive overwritten is, in fact, clean of any intelligible or prior data. This verification can be either as a separate process or included as part of the software used for overwriting.

e) Sectors not overwritten shall be identified and if they cannot be removed overwriting is not acceptable and another method must be employed.

B. 3 Degaussing

Degaussing is a process whereby the magnetic media is erased. Hard drives seldom can be used after degaussing. The degaussing method will only be used for hard drives when the drive is inoperable and will not be used for further service.

Please note that extreme care should be used when using degaussers since this equipment can cause damage to nearby telephones, monitors, and other electronic equipment. Also, the use of a degausser does not guarantee that all data on the hard drive will be destroyed. Degaussing efforts will be audited periodically to detect equipment or procedure failures. The following steps shall be followed when hard drives are degaussed:

a) Follow the product manufacturer's directions carefully. It is essential to determine the appropriate rate of coercivity for degaussing.

b) Shielding materials (cabinets, mounting brackets), which may interfere with the degaussing equipment magnetic field, shall be removed from the hard drive before degaussing.

c) Hard disk platters shall be degaussed during the degaussing process in accordance with the manufacturer's specifications.

B. 4 Physical Destruction

Hard drives shall be destroyed when they are defective or cannot be repaired or Commonwealth data cannot be removed for reuse.

a) Physical destruction shall be accomplished to an extent that precludes any possible restoration of the data. This can be attained by removing the hard drive from the cabinet and removing any steel shielding materials and/or mounting brackets and cutting the electrical connection to the hard drive unit. The hard drive should then be subjected to physical force (pounding with a sledge hammer) or extreme temperatures (incineration) that will disfigure, bend, mangle or otherwise mutilate the hard drive so it cannot be reinserted into a functioning computer.

b) Multiple holes drilled into the hard disk platters is an optional method of destruction that will preclude use of the hard drive and provide reasonable protection of data written on the drive.

C. Non-Volatile Memory Devices Data Removal Method

Electronic devices that hold data or configurations in non-volatile memory shall have all Commonwealth data removed by either the removal of the battery or electricity supporting the non-volatile memory or by such other method recommended by the manufacturer for devices where the battery is not removable. This is to include all computer equipment that has memory such as personal computers, PDAs, routers, firewalls and switches.

D. Other Electronic Media Data Removal Methods

If there is any risk of disclosure of sensitive data on media other than hard drives or devices that hold data or configurations in non-volatile memory, that media should be overwritten, degaussed or destroyed. Disintegration, incineration, pulverization, shredding or melting is acceptable means of destruction. Examples of other media include, but are not limited to, tapes, diskettes, CDs, DVDs, worm devices, and USB data storage devices.

Flash drives may be overwritten with a three pass minimum. Diskettes, CDs, DVDs, Tape backups may be degaussed or destroyed.

If overwriting or degaussing is selected, the steps for the selected method as stated in this standard shall be followed.

Burning, shredding or pulverizing of non-classified CD-ROMs by end- users is not recommended. CD-ROM discs do not require extensive destruction. Discs that are outdated or no longer needed may be rendered unreadable by cutting in half or deep scratching the data side (the shiny side without the label) with a nail, screwdriver, or similar tool. Two deep radial scratches extending from the small inner hole to the outer edge are sufficient to prevent unauthorized access to the data. These discs may be placed in the general waste stream for disposal.

E. Quality Assurance Testing of Data Removal

The effectiveness of the data removal process shall be tested by a quality assurance function independent of the organizational unit performing the data removal. The quality assurance tester

shall test for effective data removal for electronic media once the data has been removed or otherwise made unreadable.

If more than one device has had the data removed, a sample of each device type can be tested as opposed to testing every device. Individual samples should be taken for each type of electronic media (i.e. hard drives of personal computers, Personal Digital Assistants (PDAs), routers, firewalls, switches, tapes, diskettes, CDs, DVDs, cell phones, printers, and Universal Serial Bus (USB) data storage devices). The sample size for each device type should be commensurate with the sensitivity and risk of the type of data stored but must be at least 10% of the total number of devices for each type of electronic media.

The testing must be documented including date, tester(s), total number of devices in the lot, number tested, method of testing and the result. Testing must be performed within 1 week of the data removal. Test methods may include physical observation if the data removal method was physical destruction or attempting to boot up and read data if the method was overwriting. If testing of a sample reveals a failure in data removal the agency's ISO must be notified and all devices in that lot must be tested.

F. Certification

The data remover must document the data removal including certifying that the data has been effectively removed.

F.1 Steps

a) Prior to the physical disposition of the electronic media (surplusing, transfer to include reassignment within the agency, trade-in, disposal, or replacement), the following information regarding the data removal process shall be documented on a form (see: Appendix C):

1. The type of equipment/media from which Commonwealth data is being removed.
2. The date of the data removal.
3. The method(s) used to expunge the data from the storage media.
4. The name of the person removing the Commonwealth data.
5. The name and signature of the person's supervisor.

b) The form and a Certification Tag (see: Appendix A) shall be completed and signed by the person responsible for the removal of Commonwealth data. The completed form shall be maintained in a secure location and available for audit. The completed Certification Tag shall be affixed to the electronic media storing the data. For devices such as those with hard drive(s), firewalls, and PDAs, a certification tag shall be affixed to each device. For mobile media such as CDs tapes, etc. one certification may be completed for each physically aggregated lot by affixing the certification tag to the box or shrink wrapped pallet. Lots must be

aggregated when there is more than one person per function per lot (i.e., more than one data remover, or more than one quality assurance tester, etc.).

G. Maintenance and Warranty

It is necessary to protect data on computer hard drives that malfunction and require maintenance or replacement under warranty. Each agency or its service provider shall make considerations in new or renewed contracts that address the protection of COV data on hard drives for warranty or maintenance purposes. Following are standards when maintenance or warranty is necessary:

a) If the hard drive malfunctions and data can be removed in accordance with the requirements in this standard, the drive may be returned to the supplier for replacement under warranty or maintenance.

b) Hard drives that are inoperable and do not allow data to be removed in accordance with the requirements in this standard, shall be physically destroyed using a method previously outlined in B.4 Physical Destruction.

H. Data Recovery

In the event data stored on a damaged, failed, corrupted or inaccessible primary storage media cannot be accessed normally and must be salvaged, data recovery methods must be employed. If recovery of data contained on an electronic storage media is required, the agency must provide adequate controls commensurate with the sensitivity of the data contained on the storage media as follows:

a) If a third party is used to recover the data, the agency must ensure that requirements for data protection as outlined in the COV ITRM IT Security Policy and Standard are adhered to.

b) The agency shall require a non-disclosure agreement (see: Appendix B) and/or confidentiality agreement in order to strictly enforce the privacy of the data.

c) If the media must be removed from the agency premises and sent offsite for recovery, the agency must ensure and the vendor must agree to provide a secure facility and safeguarding capabilities such as background checks, etc. to address handling and processing requirements of sensitive information and that the vendor agrees to notify the agency immediately if an unauthorized party is believed to have gained access to the Commonwealth data on the media.

Resources for the Removal of Commonwealth Data from Electronic Media

VITA will maintain on its website a list of resources that according to the manufacturers' claims (which the agencies are cautioned to verify), appear to meet this Standard for the removal of data

from electronic media. The list of recommended software may be viewed at the following URL: http://www.vita.virginia.gov/library/default.aspx?id=5046

Appendix A: Certification Tags

Certification of the Removal of Commonwealth Data from Electronic Media

Section F.1.b. of this Standard requires that "The completed Certification Tag shall be affixed to the electronic media storing the data. For devices such as those with hard drive(s), firewalls, and PDAs, a certification tag shall be affixed to each device. For mobile media such as CDs tapes, etc. one certification must be completed for each physically aggregated lot by affixing the Certification Tag to the box or shrink wrapped pallet." To reduce costs and standardize tags, each agency or its service provider shall adhere to the following method for tagging equipment certified to be in compliance with this Standard.

Printing Certification Tags

Copy the Certification Tags on the following page into a standard 8.5 by 11 inch portrait orientated word document. The tags are designed to print out on standard 2 by 4 inch shipping labels (i.e., Avery Template 5163). Preferably the tags will be printed in red letters for ease of recognition; therefore if possible, each agency or its service provider will print the tags from a color printer.

To avoid tag printing errors, click your computer's Tools/Letters and Mailings/Envelopes and Labels tab and set the Labels option to "Avery standard, 5163 shipping" then practice using plain paper, holding the paper in front of a label sheet and up to the light, in order to check positioning. Most laser products are designed to work in laser printers directly from the automatic feed tray. Manual, copier and ink jet labels will not feed through consistently and may damage laser printers. To ensure proper operation, read the manufacturer's instructions that come with the shipping label before printing.

☐ **WIPED**
☐ **DEGAUSSED**
☐ **DESTROYED**
SURPLUS/ASSET TAG NO: ____________________

Removed by (PRINT NAME) DATE

SUPERVISOR SIGNATURE DATE

PRINT SUPERVISOR NAME

☐ **WIPED**
☐ **DEGAUSSED**
☐ **DESTROYED**
SURPLUS/ASSET TAG NO: ____________________

Removed by (PRINT NAME) DATE

SUPERVISOR SIGNATURE DATE

PRINT SUPERVISOR NAME

☐ **WIPED**
☐ **DEGAUSSED**
☐ **DESTROYED**
SURPLUS/ASSET TAG NO: ____________________

Removed by (PRINT NAME) DATE

SUPERVISOR SIGNATURE DATE

PRINT SUPERVISOR NAME

☐ **WIPED**
☐ **DEGAUSSED**
☐ **DESTROYED**
SURPLUS/ASSET TAG NO: ____________________

Removed by (PRINT NAME) DATE

SUPERVISOR SIGNATURE DATE

☐ **WIPED**
☐ **DEGAUSSED**
☐ **DESTROYED**
SURPLUS/ASSET TAG NO: ____________________

Removed by (PRINT NAME) DATE

SUPERVISOR SIGNATURE DATE

PRINT SUPERVISOR NAME

☐ **WIPED**
☐ **DEGAUSSED**
☐ **DESTROYED**
SURPLUS/ASSET TAG NO: ____________________

Removed by (PRINT NAME) DATE

SUPERVISOR SIGNATURE DATE

PRINT SUPERVISOR NAME

☐ **WIPED**
☐ **DEGAUSSED**
☐ **DESTROYED**
SURPLUS/ASSET TAG NO: ____________________

Removed by (PRINT NAME) DATE

SUPERVISOR SIGNATURE DATE

PRINT SUPERVISOR NAME

☐ **WIPED**
☐ **DEGAUSSED**
☐ **DESTROYED**
SURPLUS/ASSET TAG NO: ____________________

Removed by (PRINT NAME) DATE

SUPERVISOR SIGNATURE DATE

PRINT SUPERVISOR NAME

☐ **WIPED**
☐ **DEGAUSSED**
☐ **DESTROYED**
SURPLUS/ASSET TAG NO: ____________________

Removed by (PRINT NAME) DATE

SUPERVISOR SIGNATURE DATE

☐ **WIPED**
☐ **DEGAUSSED**
☐ **DESTROYED**
SURPLUS/ASSET TAG NO: ____________________

Removed by (PRINT NAME) DATE

SUPERVISOR SIGNATURE DATE

PRINT SUPERVISOR NAME

Appendix B: Non-Disclosure Agreement

CONFIDENTIALITY OF AGENCY INFORMATION:

1. Contractor shall take all precautions and measures necessary to ensure the integrity, nondisclosure, confidentiality and protection of all data and information obtained from <AGENCY NAME> or derived there from, including but not limited to all original reporting forms and data in any other form, and agrees to comply with all Federal and state guidelines including but not limited to the COV ITRM Standard SEC501-01 and the Data Protection Guideline SEC507-00 concerning the protection of sensitive data.

2. Prior to the commencement of any work for <AGENCY NAME>, the contractor shall declare in writing that he or she understands that all data and information obtained from <AGENCY NAME> or derived there from is sensitive and will be held in the strictest confidence by Contractor, its officers, directors, agents, and employees and that Contractor, its officers, directors, agents, and employees shall be governed by and comply with Federal and State laws prohibiting the disclosure of information obtained or compiled during the course of their work for <AGENCY NAME>.

3. All information obtained and work performed under this <AGENCY NAME> contract/order is considered sensitive, requires use of sensitive and personal data and information and falls under one or more categories of information that is subject to protection from disclosure and misuse, including but not limited to: personal information and highly restricted personal information in connection with motor vehicle records under the Federal Drivers Privacy Protection Act, (18 USC 2721 et seq.) law enforcement sensitive data and information, the Privacy Act, personal, vehicle and driver information as defined under and governed by Va. Code §46.2-208 et seq. and personal information as defined under and governed by the Virginia Government Data Collection and Dissemination Practices Act (VA Code §2.2-3800 et seq.).

4. All source materials/data/information and resultant work products compiled or created and any information or portion of information derived there from are the property of <AGENCY NAME> and must not be used by the contractor for any purpose other than the purpose outlined by this agreement.

5. The contractor, its officers, directors, agents and employees shall hold all information obtained under a <AGENCY NAME> contract/order in the strictest confidence. All information obtained shall be used only for the purpose of performing this contract/order and shall not be divulged nor made known in any manner to any person except as necessary to perform this contract/order. Neither Contractor, nor its officers, directors, agents, or employees shall divulge, sell, or distribute any information obtained from <AGENCY NAME> or derived there from at any point in time, even after termination or expiration of a contract/order.

6. Except as specifically authorized by the contract/order, Contractor, its officers, directors, agents, and employees are prohibited from reproducing <AGENCY NAME> source media, written products, or any portion thereof.

7. The contractor shall notify in writing, each of its officers, directors, agents, and employees having access to <AGENCY NAME> information that such information may be used only for the purpose and to the extent authorized in this contract.

8. The Contractor shall provide a security plan outlining the steps and methods taken to secure and protect the information provided by <AGENCY NAME> to address the following points:

- Security of Files and/or Copies of Records (for Hardcopy).
- Security of on-line Computer Terminals (On-Line Users Only).
- Designation of Authorized Users/Assignment of Access Codes.
- For automated interfaces/electronic extraction and storage of data, if applicable:
- Security of Records, Files, and Systems, use of encryption for storage.
- Names and addresses of data extraction method and software creators/vendors,
- Network Diagrams and descriptions of Data Extraction methods and software,
- Descriptions of system support processes including backup methods and frequencies.
- Proposed Audit/Management Controls Over Access and Dissemination of Requested Information.

9. Contractor agrees to comply with all federal and state statues, rules and regulations and understands that disclosure of any information, by any means, for a purpose or to an extent unauthorized herein, shall be grounds for immediate termination of this agreement may subject the offender to criminal sanctions.

10. Contractor shall indemnify, defend, and hold harmless the Commonwealth, <AGENCY NAME>, its officers, directors, employees and agents from and against all losses, liabilities, damages and all related costs and expenses (including reasonable attorneys' fees and disbursements and costs of investigation, litigation, settlement, judgments, interest and penalties), incurred in connection with any action or proceeding arising directly or indirectly from unauthorized use or disclosure by Contractor, its agents, directors, officers or employees, of any data or information obtained from <AGENCY NAME> pursuant to this agreement, or derived therefrom. Contractor shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of this state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, or with any measures necessary to determine the scope of the breach, identify the individuals affected, and restore the reasonable integrity of the data system. Contractor shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The

notification required may be delayed if a law enforcement agency affirmatively determines that the notification will impede a criminal investigation.

- Notice may be provided by one of the following methods:

  (1) written notice to the most recent available address the person or business has in its records;

  (2) electronic notice, if the person's primary method of communication with the individual is by electronic means, or if the notice provided is consistent with the provisions regarding electronic records and signatures in United States Code, title 15, section 7001; or

  (3) substitute notice, if the person or business demonstrates that the cost of providing notice would exceed $250,000, or that the affected class of subject persons to be notified exceeds 500,000, or the person or business does not have sufficient contact information. Substitute notice must consist of all of the following:

  (i) e-mail notice when the person or business has an e-mail address for the subject persons;

  (ii) conspicuous posting of the notice on the Web site page of the person or business, if the person or business maintains one; and

  (iii) notification by major statewide media, including newspaper, radio and television.

- If a person discovers circumstances requiring notification of more than 500 persons at one time, the person shall also notify, within 48 hours, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined by United States Code, title 15, section 1681a, of the timing, distribution, and content of the notices.

- Notification must include:

  (1) a general description of what occurred and when:

  (2) the type of PII that was involved

  (3) what actions have been taken to protect the individuals personal information from further unauthorized disclosure.

  (4) what if anything, the contractor will do to assist affected individuals, including contact information for more information and assistance; and

(5) what actions the contractor recommends that the individual take.

Appendix C: Data Removal Quality Assurance Form

Date:	
Tester(s):	
Total Number of Devices in the Lot:	
Number of Devices Tested:	
Method of Testing:	
Findings:	